

ABSTRACT OF THE DISCLOSURE

A secure method of conducting an electronic transaction over a public communications network is provided which utilizes a pseudo-expiration date in the expiration date field of an authorization request. One of the preferred methods comprises:

generating a per-card key associated with an account number;
generating a message authentication code using the per-card key;
converting the message authentication code into a pseudo expiration date;
generating an authorization request for the transaction, the request having an expiration date field containing the pseudo expiration date; and
verifying the message authentication code based on the pseudo expiration date.

Another embodiment of the invention includes a method of conducting an electronic transaction over a public communications network, with a payment account number having an associated pseudo account number, comprising:

- (a) providing the pseudo account number with a control field indicating one of a plurality of key-generation processes to be used to generate an authentication key;
- (b) generating an authentication key associated with the pseudo account number using one of the plurality of key-generation processes indicated in the control field of the pseudo account number;
- (c) using the authentication key to generate a message authentication

code specific to the transaction;

(d) generating an authorization request message including the message authentication code and the pseudo account number; and

(e) verifying the message authentication code using the indicated key-generation process and the authentication key.

0906495 062201
102290 5849350